

UNIVERSITE CATHOLIQUE DE LOUVAIN

ECOLE POLYTECHNIQUE DE LOUVAIN



# Leak sources analysis System

# Manual

Supervisor: Dr. Ramin SADRE

by Mattieu DETAILLE

& Mohammad Muntasib Ali SYED

# 1 Run your system

This document explains how to run your live leak source detection system and how to generate your leak source automated report based on pcap files (for the basic capture) and/or txt files (for the *Man in the Middle attack*). Indeed, our system allows you to perform basic capture and/or to perform a *Man in the Middle attack*. If you want more information about the leak source types captured by the system, don't hesitate to read our thesis.

If you choose to only run the live leak source detection system, you don't need to be able to generate the automated report by yourself, the network traffic captures and the report will be automatically made for you!

For the live traffic capture, the network traffic will be captured by period of 5 minutes. Your leak source automated report will thus be generated/updated automatically every 5 minutes in the *RESULT* directory.

If you want only to generate a leak source automated report based on capture files you already have, this means you won't capture any new traffic. You don't need any ODROID server for this part. You need however to install all the libraries by running the bash script *init.sh*, to update the *Safebrowsing database*[1](it can take several hours) and save it into the *database* directory and to fill the file *to_fill.py*, as stated in the *Setup.pdf* file. It is obvious that you have thus to copy the directory containing our source code on your computer...

# 2 Running your live leak source detection system

In order to run the system, execute the script *run.sh* : *bash run.sh [-h/–help] [-M/–MitM] [(-o/–overview)/(-s/–summary)/(-d/–detailed)]*

OPTIONS:

-M , –MitM Enable the Man in the Middle attack during the capture.

-s , –small Set the size of the generated report to small. Only the latest among (-s,-m,-l) will be retained.

-m , –medium Set the size of the generated report to medium. Only the latest among (-s,-m,-l) will be retained.

[1]to update the database, run : python covert_channel.py -u ; the script is in the folder *Covert Channel/*

-l , –large Set the size of the generated report to large. Only the latest among (-s,-m,-l) will be retained.

-n , –nmap Take the ip address of the device as argument. Check for open ports on the device. The device must be connected before starting the run.

-h , –help Show usage.

If you chose to perform a *Man in the middle attack*, you will have to configure your smart device in order to connect to the *HTTP Proxy* generated by the *Mitmproxy tool*.
If you have an Apple device:

- Go in your settings
- Push on Wi-Fi
- Connect to your generated Wi-Fi (*thesis* in our case)
- Push on the button *i* beside your Wi-Fi name
- Go down to the *HTTP Proxy* section
- Normally, it should be deactivated, push on Manual
- Fill the *server part* with the IP address *192.168.42.1*
- Fill the *port part* with *8888*

If you have a Samsung device:

- Go in your settings
- Push on Wi-Fi
- Connect to your generated Wi-Fi (*thesis* in our case)
- Push&Hold on the name of your generated Wi-Fi
- Select *Modify network config*
- Push on *Show advanced options*
- Go down to the *Proxy* section
- Normally, it should be deactivated, push on Manual

- Fill the *Proxy host name* part with the IP address *192.168.42.1*
- Fill the *Proxy port* part with *8888*
- Push on *Save*

Moreover, for each smart device, you have to accept a fake certificate generated by the *Mitmproxy* tool. To download and install this certificate, follow these steps:

- Connect to your generated Wi-Fi, after having configured (as explained previously) your smart device to connect to the HTTP proxy
- Run this command: *sudo mitmdump -b 192.168.42.1 -p 8888 -w mitm.txt –no-upstream-cer* on the ODROID server.
- Start a browser on the device and visit the domain mitm.it
- Click on the relevant icon to install the appropriate certificate, depending on your smart device
- That's it, you are now ready to perform your *Man in the Middle attack* against your smart device!

Don't forget, after your *Man in the Middle attack*, to deactivate your proxy. For the Apple device, go again in the *HTTP Proxy* section and change it to *Deactivated*. For the Samsung device, go again in the *network config* section and change the *Proxy* section to *None*.

If you want to perform a basic capture, don't forget to take out the *Man in the Middle attack* configuration (if you performed one before)! We have separated the basic capture and the *Man in the Middle attack* because we discovered that we lost some other leak source types when performing a *Man in the Middle attack*. It is thus better, if you want to be sure to capture all your leak sources, to perform the basic capture and the *Man in the middle attack* separately.

# 3 Generate your leak source automated report based on pcap/text files

In order to only generate your leak source automated report and thus not perform any traffic capture, execute the script *report_gen.py*. It is located in the *Report_generation* directory.

**Usage** : python report_gen.py [-h|–help] -i|–input <capture.pcap> -L|–Length <1|2|3> [-r|–rules <easyprivacy.txt>] [-M|–MitM <mitm.txt>][2]

The previous usage functions only if you have previously captured some pcap files (for the basic capture) and/or some txt files (for the *Man in the Middle attack* capture). You can perform some basic capture for obtaining the file *capture.pcap* thanks to the *Wireshark tool*. The *mitm.txt* file is a file obtained thanks to the *Mitmproxy tool*. To obtain such a file, you can run this command: *sudo mitmdump -b 192.168.42.1 -p 8888 -w mitm.txt –no-upstream-cer* on the ODROID server. To run this command, you need to setup the ODROID server, as explained in the *Setup.pdf* file. You also need to configure your smart device to perform the *Man in the Middle attack*, as stated in the 2 section.

[2]The python version is 2.7.